Securing E-Government
Network Security Update

June 19, 2002

Presented by:
Kevin Iwersen
Dept of Administration

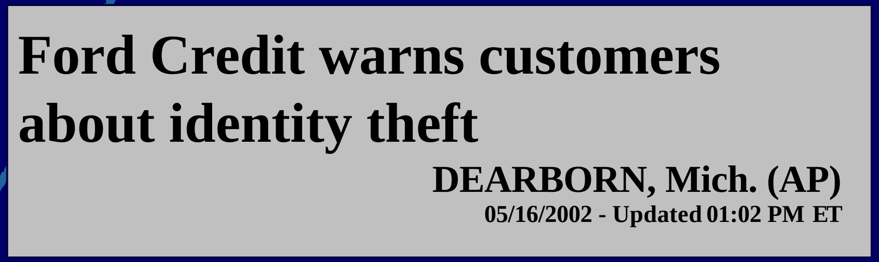
Securing E-Government

Overview

- Understanding the Threat
  - Why security?
- Highlights
  - What have we accomplished?
- Next Steps
  - Where are we headed?

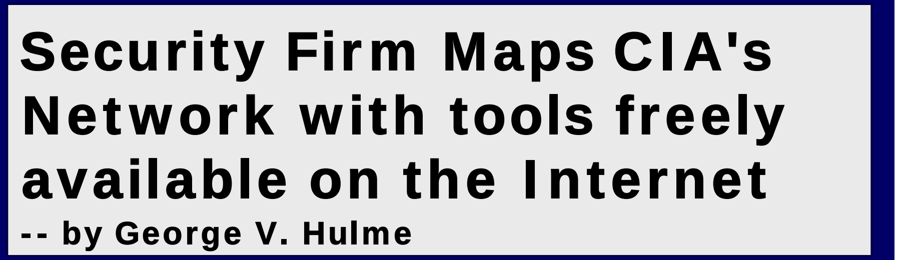
Securing E-Government

The Threat – "From the Headlines"



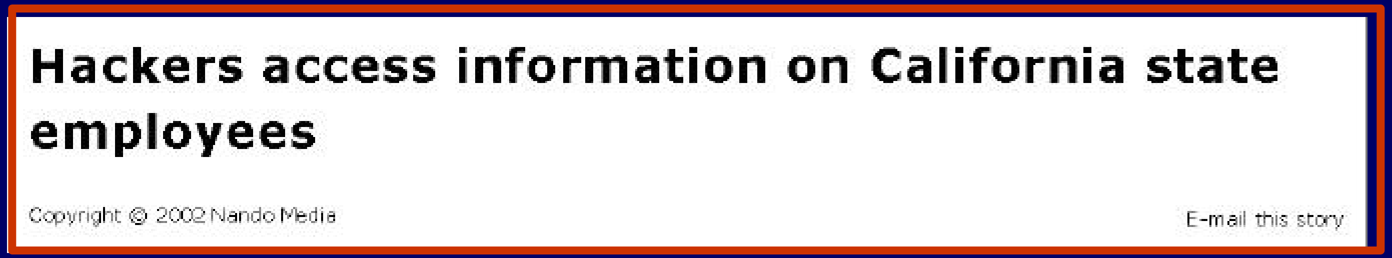
Ford Credit warns customers about identity theft

DEARBORN, Mich. (AP)
05/16/2002 - Updated 01:02 PM ET



Security Firm Maps CIA's Network with tools freely available on the Internet

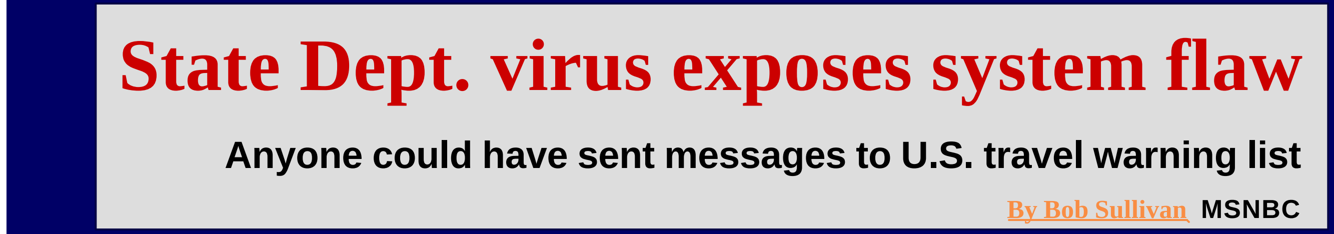
-- by George V. Hulme



Hackers access information on California state employees

Copyright © 2002 Nando Media

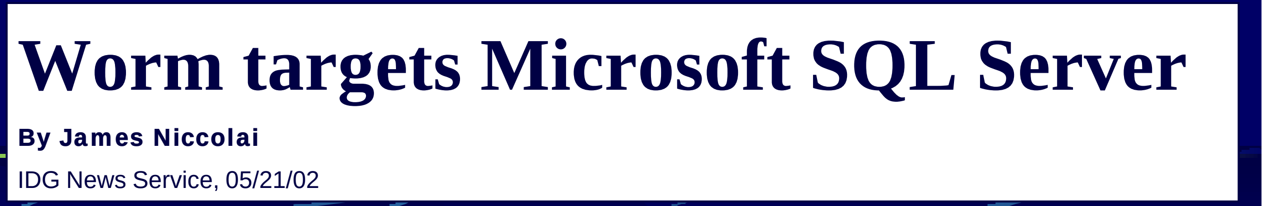
E-mail this story



State Dept. virus exposes system flaw

Anyone could have sent messages to U.S. travel warning list

By Bob Sullivan MSNBC



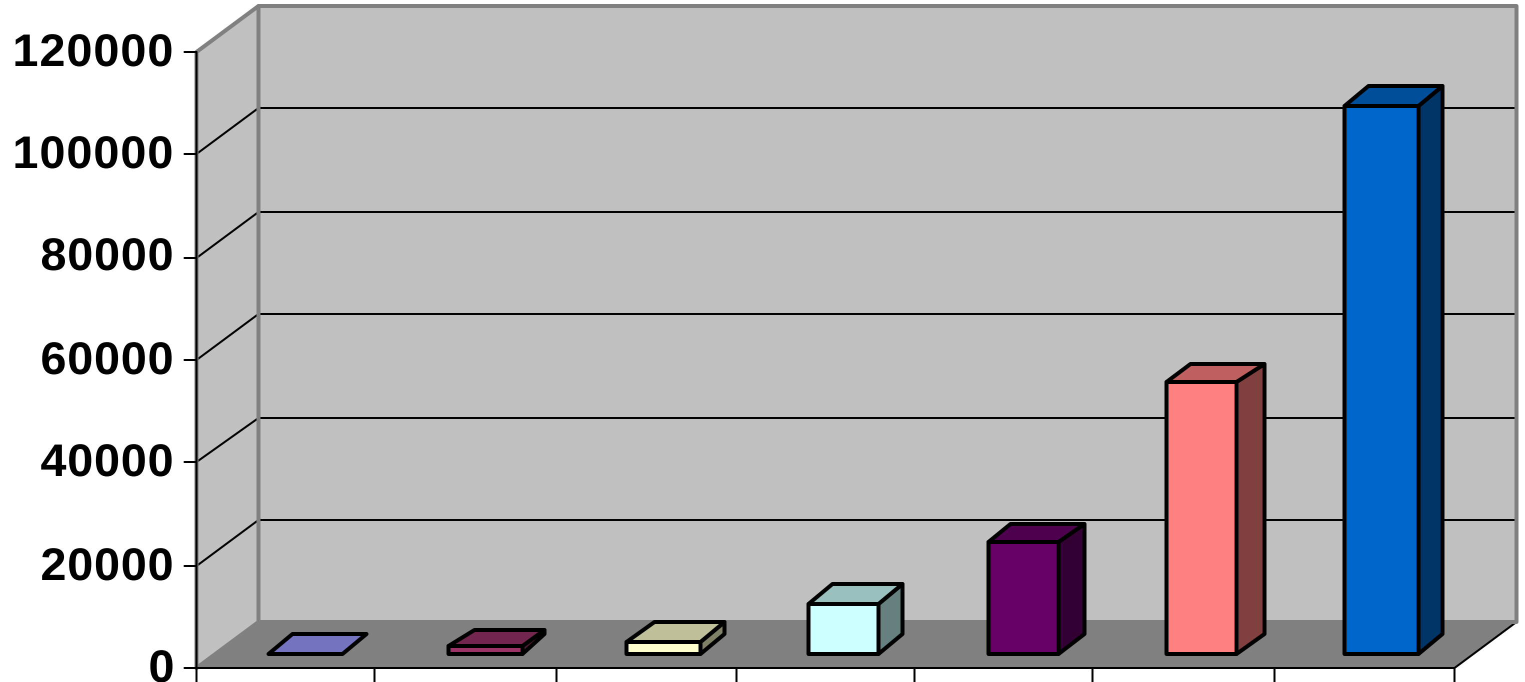
Worm targets Microsoft SQL Server

By James Niccolai

IDG News Service, 05/21/02

Securing E-Government

The Threat – Reported Incidents (CERT)

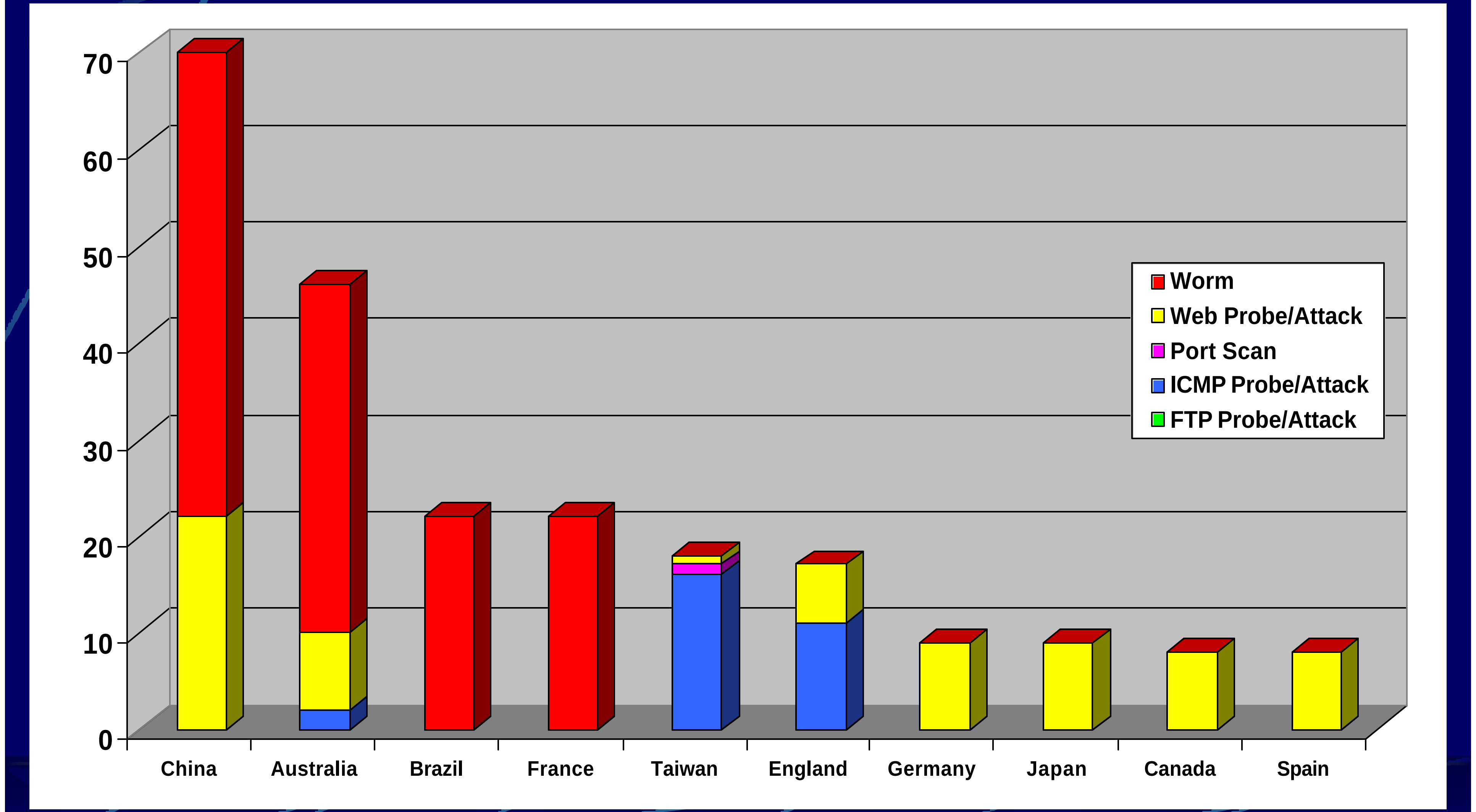


	1990	1993	1996	1999	2000	2001	2002*
Reported Incidents	252	1,334	2,573	9,859	21,756	52,658	107,316

Statistics provided by Carnegie Meillon Computer Emergency Response Team (CERT/CC)
(2002: Based on 1st Qtr Estimates)*

Threat Picture – State of Idaho's Network

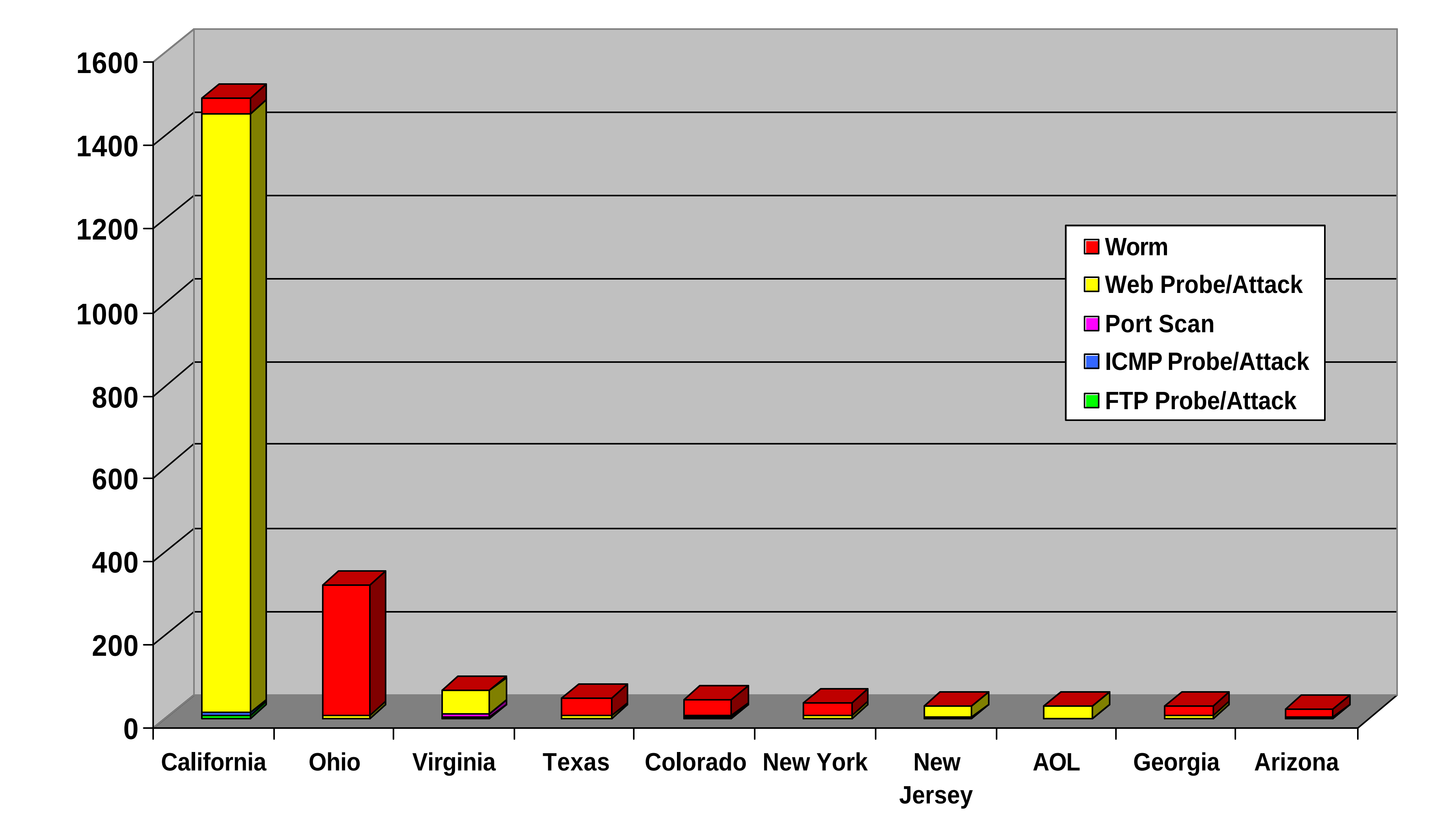
252 Overseas Attacks/Probes in 3 days



Top 10 Overseas Attack Sites – June 1 through June 3 (3 DAYS)

Threat Picture – State of Idaho's Network

2,220 U.S. Attacks/Probes in 3 days

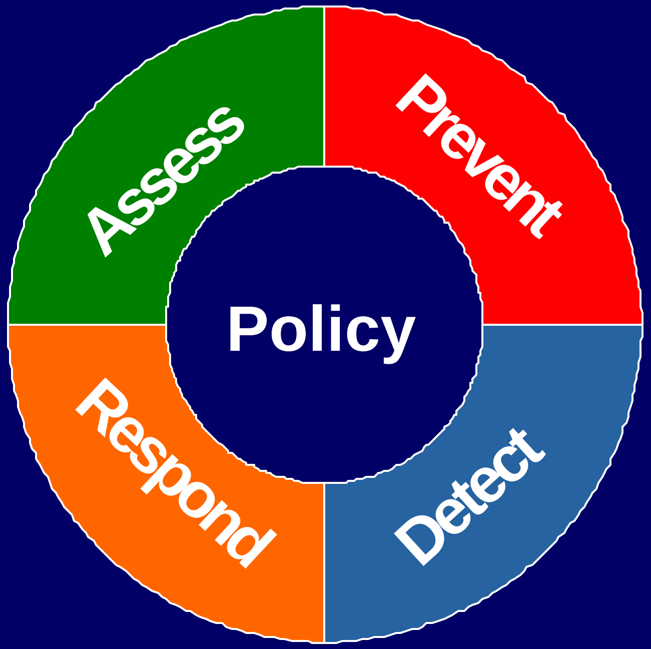


Top 10 U.S. Attack Sites – June 1 through June 3 (3 DAYS)

Our Security Philosophy

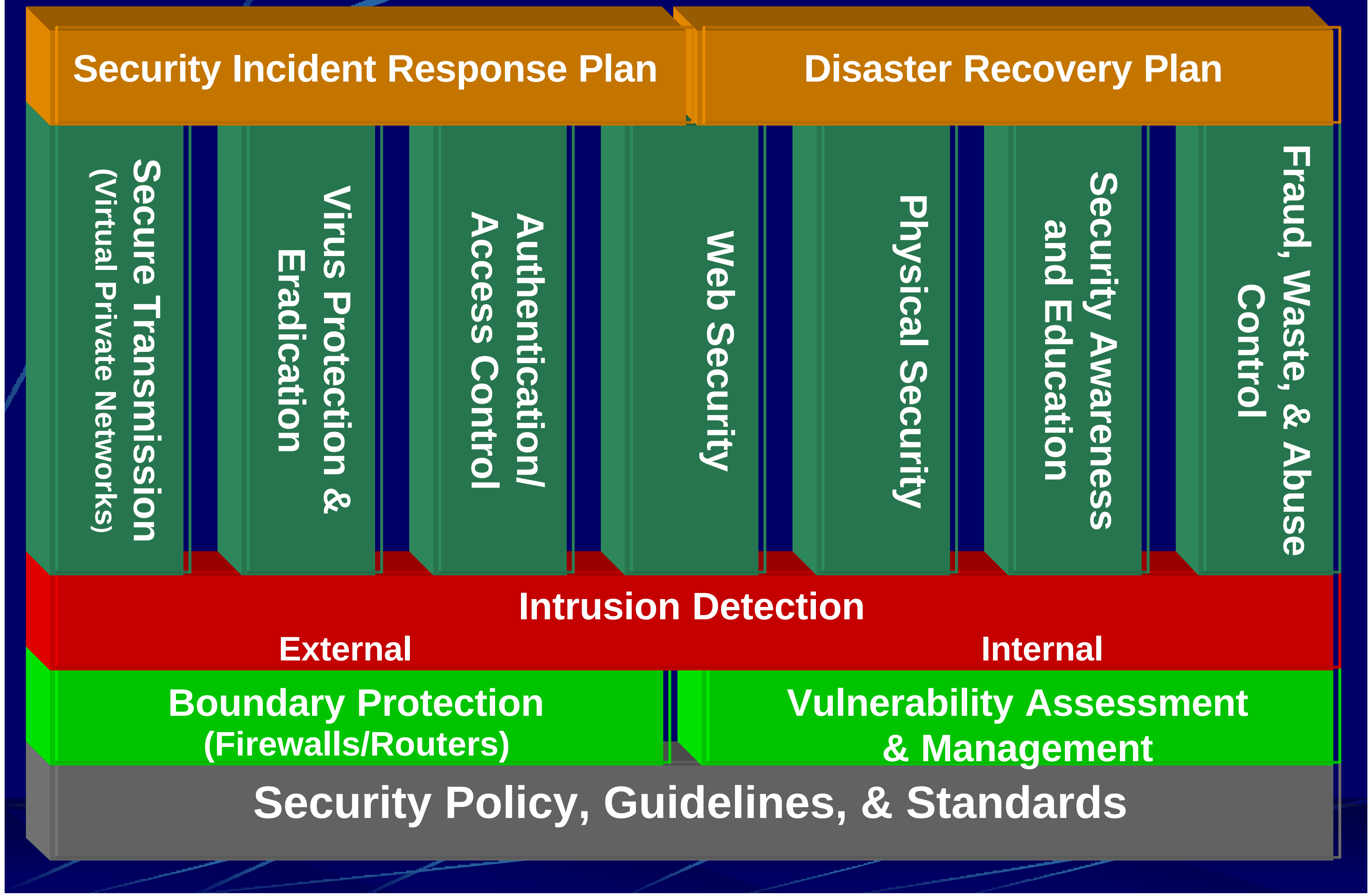
- **Defense in Depth**

- **Security Lifecycle**



How are we moving from “philosophy” to “practice”….

Security Implementation Model



Security Incident Response Plan

Disaster Recovery Plan

Secure Transmission (Virtual Private Networks)

Virus Protection & Eradication

Authentication/ Access Control

Web Security

Physical Security

Security Awareness and Education

Fraud, Waste, & Abuse Control

Intrusion Detection

External

Internal

Boundary Protection (Firewalls/Routers)

Vulnerability Assessment & Management

Security Policy, Guidelines, & Standards

Securing E-Government

Highlights (2001-2002)

- **Enterprise Anti-Virus Gateways**
  - 29,157 virus infections prevented in 7 weeks
- **Cyber Security News**
  - Periodic publication to increase security awareness
- **Disaster Recovery Plan**
  - First stage of full disaster recovery for critical WAN services
- **Managed Firewall Services**
  - Enterprise Firewalls – strong perimeter protection
  - Agency-level Firewalls – assisting with security expertise

Securing E-Government

Highlights (2001-2002)

- **Network Intrusion Detection Systems**
  - Enterprise “burglar alarm” for critical WAN connections
  - Foundation for enterprise-wide monitoring & event correlation
- **Security Web Site & Alert System**
  - Increase threat and vulnerability awareness
- **Security Product Standards**
  - Critical to interoperability, lower TCO & enterprise “views”
  - Security Products Contract in place for public agencies
- **Virtual Private Network (VPN) Services**
  - Secure communications (encrypted/strong authentication) for all State agencies

Dept of Admin Network Security

Where Are We Headed?

- **Firewall/VPN Services**
  - High Availability/Upgrades
- **Incident Response**
  - Statewide capability
- **Intrusion Detection**
  - Layered – internal & host
- **Vulnerability Assessment & Management Services**
- **Disaster Recovery**
  - “Full-Scale” Plan & Testing
- **Security Awareness**
  - Increased communication
- **Security Policies**
  - Risk Management Procedures
- **Web Security**
  - Application-level security